

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT

In re application of:

Brian E. **MARCHANT**

Application No. Not Assigned

Filed: March 30, 2001

For: SECURITY APPARATUS FOR DATA
TRANSMISSION WITH DYNAMIC
RANDOM ENCRYPTION

) Attorney Docket No. BEM1P002

) Examiner: SONG, H.

) Group Art Unit: 2131

) Date: March 30, 2001

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail to: Assistant Commissioner for Patents, Washington, DC 20231 on March 30, 2001.

Signed: 

Wanda Barton

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to substantive examination, please enter the following.

IN THE CLAIMS

Please cancel claims 1-42.

Please add the following claims.

43.(New) A data encryption apparatus comprising:

a memory that stores a racetrack array of random data and a plurality of encryption/decryption algorithms; and

a first controller operable to read said memory and to select a portion of said racetrack array based upon an array starting point and to utilize said selected portion of said racetrack array in at least one of said plurality of encryption/decryption algorithms.

44. (New) A data encryption apparatus as recited in claim 43, further comprising:

a second memory storing said racetrack array of random data and said plurality of encryption/decryption algorithms; and

a second controller operable to read said second memory and to select said portion of said racetrack array based upon said starting point and to utilize said portion of the racetrack array in at least one of the plurality of encryption/decryption algorithms.

45. (New) A data encryption apparatus as recited in claim 43, wherein said racetrack array is used to determine how many bytes of data are to be encrypted.

46. (New) A data encryption apparatus as recited in claim 45, wherein said racetrack array is used to encrypt the data by performing an ORing operation with the racetrack array data and the data to be encrypted.

47. (New) A data encryption apparatus as recited in claim 46, wherein said racetrack array is used to determine the next address used in the racetrack array.

48. (New) A data encryption system as recited in claim 47, wherein said portion of said array includes at least one byte identifying a length of data to be encrypted.

49. (New) A data encryption apparatus as recited in claim 48, wherein said portion of said racetrack array includes at least one byte identifying at least one of said plurality of encryption/decryption algorithms.

50. (New) A data encryption apparatus as recited in claim 49, wherein the starting point is different each time a lap is made around the racetrack array.

51. (New) A data encryption system as recited in claim 44, wherein said first processor includes a first controller and a first encryptor/decryptor.

52. (New) A data encryption system as recited in claim 51, wherein said second processor includes a second controller and a second encryptor/decryptor.

53. (New) A data encryption method for encrypting data wherein said data includes at least one of analog video, analog audio, digital video, digital audio and digital information, comprising the acts of;

receiving a starting address of a racetrack array of random data;

receiving data to be encrypted;

using a first portion of said racetrack array to determine how many bytes of data are to be encrypted, said first portion beginning at said starting address;

using a second through third portion of said racetrack array to determine a first and second encryption algorithms;

encrypting the determined number of bytes using the first encryption algorithm to form a first encrypted data stream; and

then encrypting said first encrypted data stream using the second encryption algorithm.

54. (New) A data encryption method as recited in claim 53, further comprising the step of using a fourth portion of said racetrack array to determine the next position on the racetrack array which will be used as said first portion of the racetrack array.

55. (New) A data encryption method as recited in claim 54, further comprising the step of determining a starting address by inputting two codes, one code from the encryptor of the data and one code from the decryptor of the data.

56. (New) A data encryption method as recited in claim 55, wherein the racetrack array and the encryption/decryption programs are stored in one memory.

57. (New) A data encryption method as recited in claim 56, wherein said encrypted data stream is decrypted with an identical racetrack array of random data.

58. (New) A data encryption method for encrypting data wherein said data includes at least one of analog video, analog audio, digital video, digital audio and digital information, comprising the steps of;

receiving a starting memory address;

receiving data to be encrypted;

using a first portion of said memory to determine how many bytes of data are to be encrypted, said first portion beginning at said starting address;

using a second through third portion of said memory to determine first and second encryption algorithms;

encrypting the determined number of bytes using the first encryption algorithm to form a first encrypted data stream; and

then encrypting said first encrypted data stream using the second encryption algorithm.

59.(New) A data encryption method as recited in claim 58, wherein said memory comprises a racetrack array of random data.

60. (New) A data encryption method as recited in claim 59, further comprising the step of starting at a different point in the racetrack array for consecutive laps around the racetrack.

61. (New) A data encryption method as recited in claim 60, further comprising the step of producing a third stream of encrypted data by subjecting a second stream of encrypted data to a third encryption algorithm.

62. (New) A data encryption method as recited in claim 61, further comprising the step of decrypting the encrypted data stream with an identical racetrack array of random data.


REMARKS

Claims 1-42 are canceled herein. New claims 43-62 have been inserted. No new matter has been added. Therefore, claims 43-62 are pending.

The above claims are directed toward the feature of a racetrack array of random data. This racetrack array performs multiple functions such as determining how many bytes of data to encrypt, what type of encryption to perform, and also provides a source of data that may be ORed with the actual data to be encrypted. See for example the discussion that begins on page 31 of the instant specification. Pages 12-13 and pages 26-28 also teach how the racetrack array is used for multiple encryption purposes. As was discussed with Examiner Chris Tucker in the parent application, the feature of the racetrack array of random data did not appear in any of the cited prior art references and would be persued in the instant case. If the Examiner feels for any reason that a telephone conference would expedite the prosecution of the case, they are encouraged to contact the undersigned at the number below.

The Applicant believes all claims are in condition for allowance and respectfully requests a timely Notice of Allowance.

Respectfully submitted,
OPPENHEIMER WOLFF & DONNELLY, LLP


Steven S. Kelley
Reg. No. 43,449

1620 L Street NW, Suite 600
Washington, D.C. 20006-5478
Telephone: (202) 312-8000
Facsimile: (202) 312-8274